CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

J-6
DISTRIBUTION: A, B, C, J, S

CJCSI 5721.01B
15 July 2002

THE DEFENSE MESSAGE SYSTEM AND ASSOCIATED LEGACY MESSAGE PROCESSING SYSTEMS

REFERENCES: See Enclosure B.

1. Purpose. This instruction provides policy, guidance, responsibilities, and information regarding the use, operation, and management of the Defense Message System (DMS).

2. Cancellation. CJCSI 5721.01A, 1 May 1999, is canceled.

3. Applicability. This policy applies to all Defense agencies responsive to the Chairman of the Joint Chiefs of Staff, Services, and combatant commands in planning, operating, managing, and using message processing systems that comprise DMS. This instruction is available to non-DOD US agencies and allied organizations for information. Copies will be provided upon request.

4. Policy

a. The policy outlined in this instruction supports the DMS goal of taking full advantage of new and evolving technology through the use of commercial-off-the shelf components and products, while reducing program costs and staffing requirements and maintaining mission-essential levels of service and security.

b. Policies pertaining to organizational message definition and processing, US Message Text Format (USMTF), and Automatic Digital Network (AUTODIN) are contained in Enclosure A.

c. Non-DOD and non-US activities must request the use of DMS in accordance with the submittal and approval process outlined in Enclosure A.

d. All data pattern traffic must be transitioned off AUTODIN in support of DMS Transition Hubs (DTHs) closure. Data pattern traffic consists of messages that are machine-generated and machine-readable. Combatant commands, Services, and agencies (C/S/As), in conjunction with the Defense Information Systems Agency (DISA) and DMS management, will determine and use alternate means for transmitting and processing affected data pattern traffic.

e. In recognition that it may be in our national interest to share classified military information (CMI) with foreign nations, the National Security Council, with approval of the President, established a national policy, National Disclosure Policy–1 (NDP-1), governing disclosure of CMI to foreign governments. Disclosure of CMI to foreign governments and international organizations is limited and will be in accordance with NDP-1 (reference a).

5. Definitions. National Gateway System. All hardware, software, policy, procedures, standards, facilities, and personnel used to exchange messages electronically and ensure messaging interoperability with allies, coalition partners, non-DOD US agencies, and other non-DOD US and foreign organizations (e.g., US defense contractors).

6. Responsibilities

a. Each combatant command will develop and implement DMS Transition Plans that include roles, responsibilities, and related implementation schedules for their headquarters.

(1) These plans must support the objectives of DMS, to include reducing costs and staffing, while meeting or exceeding mission-essential levels of service and security.

(2) These plans will identify pertinent message processing support to their component commands, non-DOD US agencies, and allied and/or coalition supporters, as necessary, to meet operational requirements. Shortfalls in messaging interoperability must be addressed with their executive agents and/or component commands.

b. J-3/DDGO/NMCS Division will develop policy and guidance for products, architectures, configurations, and capabilities that handle Single Integrated Operational Plan–Extremely Sensitive Information (SIOP-ESI).

c. The host Military Department or agency will provide tenants on base, post, camp, or station Internet Protocol router and application layer message handling services (e.g., DMS). Local host and/or tenant agreements or inter-Service support agreements may include cost recovery where appropriate.

7. Summary of Changes

a. Deleted individual messaging policy.

b. Defined National Gateway System.

c. Explained organizational message.

d. Added reference for Global Information Grid (GIG).

e. Deleted reference to Defense Information Infrastructure.

8. Releasability. This instruction is approved for public release; distribution is unlimited. DOD components (to include the combatant commands), other Federal agencies, and the public may obtain copies of this instruction through the Internet from the CJCS Directives Home Page--http://www.dtic.mil/doctrine. Copies are also available through the Government Printing Office on the Joint Electronic Library CD-ROM.

9. Effective Date. This instruction is effective upon receipt.

For the Chairman of the Joint Chiefs of Staff:

John P. Abizaid

JOHN P. ABIZAID
Lieutenant General, USA
Director, Joint Staff

Enclosures:
A -- Organizational Messaging Policy
B -- References
GL – Glossary

(INTENTIONALLY BLANK)

DISTRIBUTION

Distribution A, B, C, and J plus the following:

	Copies
Commander, US Element North American Aerospace Defense Command (NORAD)	2
Commander, Joint Interoperability Test Command (JTIC)	2
Chairman, Inter-American Defense Board	2
United States National Military Representative (USNMR) to Supreme Headquarters Allied Powers, Europe (SHAPE)	2
United States Representative to the Military Committee (USREPMC) (NATO) Liaison Office	2
United States Liaison Officer (USLO) to Supreme Allied Commander, Atlantic (SACLANT)	2
Chairman, Intelligence Community Defense Message System Management Office (ICDMO)	2

(INTENTIONALLY BLANK)

ENCLOSURE A

DEFENSE MESSAGE SYSTEM POLICY

1. Defense Message System Description. DMS relies primarily on the Defense Information System Network (reference b) Transmission Control Protocol/Internet Protocol networks: Non-Secure Internet Protocol Router Network (NIPRNET), SECRET Internet Protocol Router Network (SIPRNET), and Joint Worldwide Intelligence Communications System (JWICS) for transport. It consists of all hardware, software, policy, procedures, standards, facilities, and personnel used to exchange messages electronically between DOD organizations in a fixed location or tactical environment. DMS requirements are detailed in reference c.

2. Organizational Messaging. Organizational messaging (High-Grade DMS Service) includes command, control, communications, computers, and intelligence messages exchanged between organizational elements. These messages require approval for transmission by a designated official, are directive in nature, commit resources, make formal requests, and/or provide command position. Organizational messages must be signed and encrypted in order to provide audit and/or trace capability and nonrepudiation.

3. US Message Text Format. The Military Services, combatant commands, Joint Staff, combat service support commands, and those other activities and agencies responsive to the Chairman of the Joint Chiefs of Staff will use USMTF for all organizational messaging. USMTF provides an integrated, global secure communications and information process that can accommodate the widest range of missions and operational environments. USMTF is a single character-based messaging information structure, or syntax, and provides consistent data representation for the exchange of information among the military forces and supporting agencies of the Department of Defense. Other DOD agencies are encouraged to do the same (reference d).

4. DOD Organizational Messaging Infrastructure

a. Automatic Digital Network. AUTODIN is the legacy DOD messaging system. AUTODIN was developed in the 1960s and has been used by the Department of Defense for the exchange of organizational messaging for the past 40 years. AUTODIN consisted of a series of switching centers that processed and routed message of all classifications and caveats.

(1) Currently, three switching centers remain that provide support for organizational message users until they are transitioned to DMS or other systems. The Defense Planning Guidance (reference e) mandated that AUTODIN be phased out by 30 September 2003.

(2) AUTODIN legacy format support is achieved through the three remaining switches, referred to as DTHs, and the Pentagon Telecommunications Service Center. DTHs provide legacy switching functionality and translation services for all users. Legacy format support switching and translation will be achieved in the post-DTH architecture through the National Gateway system. DTH also provides legacy messaging for the Emergency Action Message (EAM) community. The EAM Hybrid solution, when implemented, will transition all EAM traffic off DTH circuits.

b. EAM Hybrid Solution. The EAM Hybrid Solution consists of legacy and evolutionary systems: Defense Improved Emergency Message Automatic Transmission System, Replacement Command and Control Terminal EAM injection system (known as DIRECT), the Air Force's Strategic Automated Command Control Systems, the Navy's Nova messaging systems, the DMS, and the Pentagon Telecommunications Service Center. The US Military Communications Electronics Board approved the EAM Hybrid Solution in November 2000. The EAM Hybrid Solution is expected to be operational in spring 2003.

c. Defense Message System

(1) DMS is structured to provide an interoperable, seamless, and secure writer-to-reader electronic messaging system for organizational users within the Department of Defense (both strategic and tactical). DMS uses commercial products for drafting, coordinating, and releasing messages. Today, DMS is the DOD system of record for all non-special category and/or special handling designator general service (GENSER) organizational message traffic. In the future, DMS is expected to become the DOD system of record for all organizational message traffic at all levels of classification and access (reference f).

(2) DMS components are based on the internationally developed ITU-T-X.400 message handling and X.500 directory service systems. DMS management is also based on standards and protocol developed through international forums (e.g., X.700-based Common Management Information Protocol and Internet-based Simple Network Management Protocol version 2). Multilevel Information System Security Initiative security mechanisms and Message Security Protocol, developed by the

National Security Agency (NSA), provide DMS security services to ensure the protection of DOD unclassified and classified information.

(3) DMS infrastructure is broken into two broad areas, backbone and local. DISA will acquire, operate, and maintain the DMS backbone infrastructure for the Department of Defense. Services and agencies will acquire, operate, and maintain DMS Local Control Center(s) for the user.

5. Authorities

a. Defense Information Systems Agency. As the lead agency for the Joint DMS Program, the Director, DISA, exercises program management oversight in accordance with DODD 5000.2-R (reference g). This oversight consists of adhering to the requirements for a joint program, to include system design, engineering, acquisition, implementation, integration, operational direction, and management control over all elements of DMS as a GIG component per reference h. Additionally, DISA is responsible for the design, development, testing, and maintenance of all DMS infrastructure (backbone) products. DISA responsibilities include, but are not limited to, life-cycle support and management, configuration control, and technical refresh of user components and products. User products and descriptions can be found at DISA's public web site (reference i).

b. Joint Interoperability Test Command. The Commander, JITC, administers DMS developmental, integration, and operational testing per reference h.

c. Combatant Command, Services, and Agencies. C/S/As will field, operate, and maintain DMS components and associated message processing systems within their domains. C/S/As must also obtain the necessary approval for employment of DMS components and products being connected to the local enterprise network transport layers (NIPRNET, SIPRNET, or JWICS).

d. Joint Staff, Directorate of Operations. The Joint Staff J-3 is the approving authority for declaring the EAM Hybrid Solution acceptable and the system of record for EAM dissemination. Additionally, roles and responsibilities for the C/S/As are outlined in reference j.

6. Security. Security approvals, in accordance with the DMS Capstone Test and Evaluation Master Plan (reference k), will be the joint responsibility of the NIPRNET, SIPRNET, and JWICS designated approval authorities (DAAs).

a The National Security Agency (NSA) will approve products, architectures, configurations, and capabilities that handle and support critical communications information. Additionally, NSA will exercise program management, system design, and acquisition over information assurance elements of the DMS program per reference g.

b The Defense Intelligence Agency will approve products, architectures, configurations, and capabilities that handle and support sensitive compartmented information (SCI). SCI data on information networks will be protected in accordance with ref l.

c DISA will approve products, architectures, configurations, and capabilities that handle GENSER information, not including SIOP-ESI.

d Joint Staff (J-3/DDGO/NMCS Division) will approve products, architectures, configurations, and capabilities that handle SIOP-ESI information.

(1) Per DMS Security Policy (reference m) and DMS Trusted Facility Manual (reference n), security protection is required for all messaging products at all classification levels. DMS messages will be protected by NSA-approved security protection mechanisms. Overall adequacy of security protection is determined for each DMS product by the DAAs.

(2) Each C/S/A operating a DMS GENSER user product will accredit that product, in accordance with local procedures, based upon DISA's and/or NSA's Type Accreditation for that product. DISA will ensure that all DOD Information Technology Security Certification and Accreditation Process requirements are met (reference o).

(3) Accreditation of DMS implementation and operation on SCI networks will be in accordance with applicable Department and Agency procedures for certifications and accreditation of SCI systems.

(4) The Joint Staff and C/S/As are responsible authorities for determining users with a need to process SIOP-ESI messages (reference p). The Director, Joint Staff, is the DAA for all SIOP-ESI accreditation. J-3/DDGO/NMCS Division is the executive agent for all Joint Staff SIOP-ESI DAA actions.

7. Approval Procedures for DMS Services for Non-DOD Activities

a. US Government non-DOD organizations may be considered for DMS services, upon OSD approval, if any of the following conditions exist:

(1) The requirement is considered command and control and cannot be satisfied by other means.

(2) The requirement supports a DOD mission.

(3) Other justification as deemed appropriate by OSD.

b. US non-Government organizations may be considered for DMS services, upon OSD approval, if any of the following conditions exist:

(1) They are sponsored by a DOD activity.

(2) Their requirement is in direct support of a DOD mission.

(3) Other justification as deemed appropriate by OSD.

c. Non-US activities may be considered for DMS services. Requests will be processed under the provisions of reference q. As appropriate, OSD will direct DISA to effect or facilitate implementation.

8. DMS Transition Plan for Non-DOD Activities. DISA will take action through the DMS management structure to ensure that all non-DOD, non-Government, and non-US activities are notified of DMS planning. In particular, DISA will ensure that non-DOD activities currently receiving baseline AUTODIN services are addressed in all aspects of the DMS transition planning.

(INTENTIONALLY BLANK)

ENCLOSURE B

REFERENCES

a. CJCSI 5221.01, 6 April 1999, “Delegation of Authority to Commanders of Combatant commands to Disclose Classified Military Information to Foreign Governments and International Organizations”

b. CJCSI 6211.02, 22 May 1996, “Defense Information System Network and Connected Systems”

c. Multicommand Required Operational Capability (MROC), 3-88, Change 2, 31 October 1997, "Defense Message System"

d. CJCSI 6241.02, 31 July 1996, “United States Message Text Formatting Policy and Procedures”

e. Office of the Secretary of Defense, April 2000, “Defense Planning Guidance, FY 2002 – 2007”, Part III Guidance, Prepare Modernization, Information Superiority, Program Guidance, Communications, page 109, paragraph 11

f. Assistant Secretary of Defense (ASD) for Command, Control, Communications, and Intelligence (C3I) memorandum, 12 April 2001, “Update to the Revised Defense Message System Transition Plan”

g. DODD 5000.2-R, 10 June 2001, “Mandatory Procedures for Major Defense Acquisition Program (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs”

h. DODD 5105.19, 25 June 1993, "Defense Information Systems Agency (DISA)"

i. DISA, Web site, “Core Products”[1]

j. Joint Staff, 5 October 2001, “Emergency Action Message Hybrid Solution Management Plan”

k. DISA, current edition, "Defense Message System (DMS) Revised Capstone Test and Evaluation Master Plan (DMS TEMP)"

[1] http://disa.dtic.mil/apps/apm/

l. Director Central Intelligence, Directive 6/3, 5 June 1999, “Protecting Sensitive Compartmented Information within Information Systems”

m. DISA, 19 March 1999, “DMS Security Policy”[2]

n. DISA, Working Draft, 24 June 2000, “DMS Trusted Facility Manual”[2]

o. DODD 5200.40, 30 December 1997, “DOD Information Technology (IT) Security Certification and Accreditation (C&A) Process (DITSCAP)”

p. CJCSI 3231.01, SECRET, 7 January 2000, “Safeguarding the Single Integrated Operational Plan”

q. CJCSI 6740.01, 18 September 1996, "Military Telecommunications Agreements and Arrangements Between the United States and Regional Defense Organizations or Friendly Foreign Nations"

[2] https://dms-ca.dtic .mil/d2/dms/invited/

GLOSSARY

ABBREVIATIONS AND ACRONYMS

AUTODIN	Automatic Digital Network
CD-ROM	Compact Disc–Read Only Memory
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CMI	classified military information
C/S/A	combatant command, Service, and agency
DAA	designated approval authority
DISA	Defense Information Systems Agency
DMS	Defense Message System
DODD	Department of Defense Directive
DTH	Defense Message System (DMS) Transition Hub
EAM	Emergency Action Message
GENSER	general service
GIG	Global Information Grid
JWICS	Joint Worldwide Intelligence Communications System
NDP-1	National Disclosure Policy–1
NIPRNET	Non-Secure Internet Protocol Router Network
NSA	National Security Agency
OSD	Office of the Secretary of Defense
SCI	sensitive compartmented information
SIOP-ESI	Single Integrated Operations Plan-Extremely Sensitive Information
SIPRNET	SECRET Internet Protocol Router Network
USMTF	United States Message Text Format

(INTENTIONALLY BLANK)